Corporation for National and Community Service

Policies and Procedures

Policy Number: 367 **Effective Date:** April 19, 2017

Subject: Cybersecurity Policy

Purpose: This policy is designed to protect CNCS information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction.

Who is Covered: This policy applies to all CNCS employees, including federal full-time, part-time, and temporary employees, contractors, interns, volunteers, or any other individual who operates or has access to CNCS information or information systems.

Originating Office: OIT

Summary of Revisions: Removed and added roles and responsibilities and added information about cloud computing.

Approved By:

Mikel Herrington
Acting Chief of Staff

If you need this document in an alternative format, please contact the Administrative Services Help Desk at 202/606-7504 (voice) or 800-833-3722 (TDD). You may also send an email to ashelp@cns.gov

Table of Contents

1.0 CYBERSECURITY PROGRAM

The Corporation for National and Community Service (CNCS) is responsible for implementing and administering a cybersecurity program. This program must protect CNCS information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction. CNCS's procedures for securing federal information must be consistent with federal security and privacy laws and policies (see Appendix A: Applicable Laws and References). To meet these requirements, CNCS has established a Cybersecurity Program to secure information systems and protect privacy information. This policy documents and describes the cybersecurity program. It is reviewed and updated annually, or as needed.

1.1. Objective

The objective of this policy is to establish a Cybersecurity Program that:

- Protects and provides adequate security for privacy, business sensitive information and any information created, collected, processed, stored, transmitted, disseminated, or disposed of by or on behalf of the agency, to include Federal information residing in contractor information systems and networks
- Implements best security practices based on a risk and cost/benefit approach
- Provides training and awareness for users, employees with elevated privileges, and those with information assurance roles

1.2. Scope

This policy applies to:

1. CNCS information systems (IS) (internal or contractor managed), contracted information technology (IT) services, or any IS that creates, collects, uses, processes, stores, maintains, disseminates, discloses, transmits or disposed of CNCS information.
2. Any information system funded by CNCS, all information systems connected to CNCS information systems, and prototype information systems connected to any CNCS operational information systems; and
3. Agency employees, contract personnel, and other users of CNCS information and information systems under written agreement between the user, contract personnel or trusted third party and CNCS.

1.3. Noncompliance

Any user found using a CNCS system outside of defined privileges could be subject to loss or limitations on use of information resources[1], as well as disciplinary and/or legal action, up to termination of employment and referral for criminal prosecution.

[1] A CNCS information resource is any information (e.g. files, data, etc.), system, application or service that a CNCS employee or contractor can access.

2.0 ROLES AND RESPONSIBILITIES

The following sections describe the roles and responsibilities of key participants involved in the Cybersecurity Program. Some of the following positions may be held by the same individual if there is not an oversight function, and some may be held by more than one individual if there is a clear delineation of responsibility.

2.1. Chief Executive Officer (CEO)

The CEO is responsible for ensuring that the Cybersecurity Policy is developed and implemented in accordance with regulatory and business requirements. The CEO plays a crucial role in allocating resources and fostering commitment to the Cybersecurity Program. In support of the Cybersecurity Program, the CEO ensures that the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) positions are filled with qualified individuals.

2.2. Chief Information Officer (CIO)

The CIO[2] is responsible for the execution of CNCS's overall Information Technology (IT) program and has delegated authority to the CISO for the management of the Cybersecurity Program. The CIO is the focal point for IT management and governance of IT portfolios and is responsible for:

- Designating a CISO to develop and maintain an agency-wide cybersecurity program in accordance with the Federal Information Security Modernization Act of 2014 (FISMA)[3]
- Assisting senior agency officials with their security responsibilities
- Overseeing personnel with significant responsibilities for information security and ensuring that personnel are adequately trained
- Coordinating with senior management to report annually to the CEO on the overall effectiveness of CNCS's Cybersecurity Program, including progress of remedial actions
- Allocating resources dedicated to protecting the agency's mission and business functions against known and emerging cyber threats in the most timely and cost-effective manner
- Ensuring that information systems are covered by approved system security plans (SSPs) and are authorized to operate
- Ensuring an agency cybersecurity program is effectively implemented
- Keeping the agency's senior executives abreast of the CNCS' cyber capabilities, and informing them in the event of any attacks

[2] Because the position of CISO involves the exercise of inherently governmental authority, the individual in this position must be a federal government employee.

[3] 44 U.S. Code § 3544.

- Establishing and supporting the resource and budget requirements to meet the intent of this policy

2.3. Chief Information Security Officer (CISO)

The CISO[4] carries out the CIO's security and privacy responsibilities under the Federal Information Security Modernization Act 2014 (FISMA), and other laws, policies, and regulations listed in APPENDIX A:Appendix A: Applicable Laws and References and is responsible for managing the Cybersecurity Program. The CISO must: (i) possess and maintain professional qualifications, including training and experience, required to administer the cybersecurity functions; (ii) maintain cybersecurity duties as a primary responsibility; and (iii) head an office with the mission and resources to assist the organization in achieving adequate security[5] of its information and information systems. The CISO is responsible for:

- Developing an agency-wide Cybersecurity Program that provides adequate security for all CNCS electronic information and information systems
- Advising and updating senior management on the effectiveness of the Cybersecurity program
- Work with senior management to ensure IT security protection policies are accepted, implemented, reviewed, maintained and governed effectively
- Supervising compliance with the Corporation's security policies, standards and procedures
- Ensuring that personnel with significant system security responsibilities are adequately trained
- Centralized reporting of information security-related activities. Reporting duties include but are not limited to developing and submitting an annual FISMA report and reporting security incidents to US-CERT
- Monitoring the corrective actions taken in response to a security incident and assigning resources when required
- Auditing existing systems and providing comprehensive risk assessments
- Keeping abreast of the latest security threats and security posture of CNCS network and information systems
- Ensuring that changes to infrastructure and applications do not compromise the security of the agency beyond an acceptable risk

[4] Because the position of CISO involves the exercise of inherently governmental authority, the individual in this position must be a federal government employee.

[5] 'Adequate security' means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

- Educating and providing consultation for CNCS personnel to comply with cybersecurity requirements and protect CNCS assets

2.3.1. Chief Privacy Officer (CPO)[6]

The Chief Privacy Officer carries manages the privacy program on behalf of the Senior Agency Official for Privacy (SAOP). Below describes the CPO responsibilities as it relates to cybersecurity.

- As a designee the CPO, shall manage privacy risks associated with any agency activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personal identifying information (PII) by programs and information systems
- The CPO's review of privacy risks shall begin at the earliest planning and development stages of agency actions and policies that involve PII, and continue throughout the life cycle of the programs or information systems
- Select and implement privacy controls based on agency's privacy requirements and the need to protect PII
- Coordinate privacy control selection and implementation with mission and business owners, and the CISO/CIO
- Implement the optional control enhancements when there is a demonstrated need for additional protection
- Document outcomes of Privacy Impact Assessments (PIA) and system of records notices (SORNs)
- CPO shall ensure ongoing collaboration between CISO and the SAOP to ensure coordination of security and privacy activities

2.4. Contract Officer Representative (COR)

An assigned COR shall ensure that all policies, procedures, or guidelines are enforce on responsible contracts to include:

- Verify the contract and determine if the system is a covered contractor[7] information system and has the proper FAR clause language to cover vendor requirements to implement a set of cybersecurity measures to attain the basic safeguarding security and privacy controls in accordance to FAR part 52.204-21, NIST SP 800-171, FISMA of 2014 and other applicable statutory, regulatory and policy requirements

[6] The CISO shall also carry the responsibilities as Chief Privacy Officer, unless and until another designation is made by the CEO.

[7] A covered contractor information system is an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

- Identify if the contracted service is in a cloud environment. See Cloud Computing for more information
- Ensure any contractor that either accesses a CNCS system or CNCS information completes annual cybersecurity and privacy training. See Awareness and Training (AT) for more information
    - Provide a list of all personnel assigned to the contract and their last cybersecurity and privacy training date. The COR will send that to cybersecurity@cns.gov with the contract number

2.5. Program Managers / Supervisors

Program managers and supervisors are responsible for the following:

- Ensuring all CNCS users under their responsibility complete initial/annual cybersecurity training and sign the CNCS Rules of Behavior on an annual basis
- Notifying OIT and/or applicable information system account managers in a timely manner when:
    - Accounts are no longer required
    - Users are terminated or transferred to another position
    - Users are out of the office for more than 30 days
    - Individual information system usage or need-to-know changes

3.0 INFORMATION SYSTEM SECURITY

3.1. Scope

CNCS must ensure that security controls are implemented considering the risk and magnitude of the harm that would result from loss, misuse, denial of service, unauthorized access, or modification of CNCS and contractor information assets.

Control families are defined in the NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, as amended. CNCS information systems must have documented procedures for each control family that explains how security controls are implemented. Procedures must be properly maintained to include reviewing and updating at least annually or whenever changes occur. The following sections provides an overview the CNCS policies, procedures, and/or programs associated with each security control family. Details pertaining to organizationally defined requirements are included in the *CNCS Cybersecurity Control Families* document.

3.2. Control Noncompliance

Waivers and/or risk acceptance for delaying, modifying, or not implementing a control must be submitted to the CISO, CIO, or delegated representative for decision or guidance. Details pertaining to noncompliance are located in the Plan of Actions and Milestones (POAM) standard operating procedures (SOP)

3.3. Information Security Controls

CNCS information systems, to which it has control, must meet the minimum security requirements which are defined in FIPS 200 "*Minimum Security Requirements for Federal Information and Information Systems*." CNCS will meet the minimum security requirements by selecting the appropriate security controls and assurance requirements as described in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. The agency will apply the baseline security controls to more closely fit its mission requirements and operational environments. The controls selected or planned must be documented in the System Security Plan.

Documents identified in this section are accessible from the COO: Office of Information Technology: Cybersecurity – Important Links: Cybersecurity Policies, SOPs and Template SharePoint page, CNCS Policies SharePoint page or the internet.

3.3.1. Program Management (PM)

The program management controls are implemented at the organizational level and are addressed through the *CNCS Cybersecurity Control Families*, this policy and other relevant documentation.

3.3.2. Access Control (AC)

Access to CNCS information resources will be limited to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. Please refer to *CNCS Cybersecurity Control Families* for further details regarding established CNCS access control measures.

3.3.2.1 Acceptable Use

All CNCS users must read, sign and comply with the CNCS Rules of Behavior (ROB) prior to gaining access to CNCS systems and resources, and re-sign annually. The intent of the ROB is to provide guidance for all CNCS employees, contractors, interns/temporary employees, and volunteer personnel concerning information security and privacy. By signing the ROB, users certify they have completed all required user training, and have read and understood the Cybersecurity ROB agreement.

All privileged users[8] must read, sign and comply with the CNCS Privileged Users Agreement and Rules of Behavior and read and re-sign it annually.

3.3.3. Awareness and Training (AT)

FISMA requires each federal agency to provide mandatory annual information security training and privacy to all personnel, including contractors involved in the use or management of federal computer systems. Further, the Office of Management and Budget (OMB) Circular A-130, requires that such training be completed prior to the granting of access to an information system.

CNCS provides this required security and privacy awareness training to all CNCS users, including senior executives, managers, and contractors prior to granting network access, and annually thereafter. Table 1: CNCS Contractor Training Requirements provides guidance to CORS concerning whether a CNCS contractor must complete the CNCS Cybersecurity Training.

Table 1: CNCS Contractor Training Requirements

The contractor has access to the CNCS network or sensitive information…	AND they have an active CNCS network account	They must complete the CNCS Cybersecurity Training and acknowledge the User Rules of Behavior (ROB)
If the contractor has access to CNCS sensitive information via a CNCS system (e.g. eSPAN,	But they **DO NOT have an active CNCS network account**	**Their company provided cybersecurity and privacy training meets the annual**

[8] Privileged user is defined as "a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform [CNSSI 4009]."

Momentum, AmeriCorps Health or Childcare Benefits, etc.)…		**training requirement. Please refer to** Contract Officer Representative (COR) **for additional information.**

Users with elevated privileges, referred to as privileged users, will be provided enhanced security training applicable to their role as a privileged user. Additionally, users assigned a specific cybersecurity role for CNCS systems, (e.g. ISO, ISSO, etc.), will be provided security role-based training.

Refer to Table 2: Cybersecurity Training Requirements for a description of the different training provided by CNCS.

Table 2: Cybersecurity Training Requirements

Type	Objective	Required Participation
Cybersecurity User Training, including Privacy and Phishing	Understanding of information security and privacy policies	All
Role Based Cybersecurity Training	Provide users with significant cybersecurity responsibilities an understanding of their roles and responsibilities for ensuring information systems operates at acceptable level of risk.	Individuals with program level security roles[9]
Privileged User Training	Provide privileged users an understanding of their roles and responsibilities as a privileged user, and the importance of safeguarding access to CNCS system resources	Individuals with elevated program/system level roles

3.3.4. Audit and Accountability (AU)

Audit logs are used to investigate security incidents, monitor any and all use of CNCS resources, provide accountability for transactions, track system changes, and assist in detection of system anomalies. CNCS audit logs for information systems must be reviewed, maintained and archived. Audit trails must provide sufficient information to, at a minimum, establish the type of event, when the event took place (i.e. date and time), where the event occurred, the source of the event, and the outcome of the event. Please refer to the *CNCS Cybersecurity Control Families* for further details regarding established CNCS audit control measures.

[9] Program levels roles include: CIO, CISO, AO, ISO, ISSO, and system/software developers, these roles are defined in the IT Risk Management Framework (RMF) Guide.

3.3.5. Certification, Accreditation, and Security Assessments (CA)

CNCS will perform security assessments [10]of information systems under its control in accordance with the FISMA of 2014.[11] CNCS will adhere to NIST security authorization guidance as set forth in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, as amended, and any applicable subsequent publications or requirements.

As stated in NIST 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, "initial system authorization is based on evidence available at one point in time, but systems and environments of operation change." To address the needs of constantly changing environments, CNCS shall adopt ongoing authorization (OA), which involves shifting from periodic to ongoing assessments and facilitates a continual state of awareness. As current system authorizations expires, an OA will be issued upon completion of its security assessment. During the first year of the OA, the Authorizing Official (AO) for the system will receive quarterly updates on the security posture of the system.

Please refer to the *CNCS Cybersecurity Control Families* for further details regarding established CNCS measures for assessment and authorization procedures.

3.3.6. Configuration Management (CM)

CNCS will establish and maintain baseline configurations and an inventory of all information systems that are operated by or under the control of the agency throughout the system development life cycle (SDLC) and establish and enforce security configuration settings for information technology products employed for an information system. Changes to each CNCS information system will be systematically planned, reviewed for security impact, approved, tested and documented at a level appropriate with the size, complexity, and sensitivity of the system.

Please refer to the *CNCS Cybersecurity Control Families* for specific details and procedures regarding established CNCS measures for configuration management and change control.

3.3.7. Contingency Planning (CP)

CNCS has developed and formally documented a contingency planning policy, *CNCS Continuity of Operations Plan (COOP)*, as amended. The COOP is reviewed annually and updated, as necessary, to ensure it is applicable to the CNCS environment and compliant with applicable federal laws, directives and policies, regulations, standards, and guidance.

The COOP outlines the major activities CNCS will perform to ensure it can maintain or resume operations within a reasonable time during and after a wide range of emergencies, including

[10] Security assessments are conduct in accordance with the Standard Operating Procedures (SOP) CS0102 Cybersecurity: Security Assessment and Authorization (SA&A)
[11] 44 U.S. Code § 3544(b)(1).

localized acts of nature, accidents and technological failures, or attack-related emergencies. CNCS information systems that support COOP related functions will define their contingency requirements in the system security plan (SSP) or other related documentation. .

Please refer to the *CNCS Continuity of Operations Plan (COOP)* for specific details regarding CNCS established policy and procedures for contingency and disaster recovery and the *CNCS Cybersecurity Control Families* for further details regarding established CNCS measures for contingency planning.

3.3.8. Identification and Authentication (IA)

CNCS will establish unique identifiers, e.g. user name and password, for all CNCS users accessing CNCS information resources. The specific method(s) of authentication used for each system shall be commensurate with the level of sensitivity of the system to be accessed (i.e. more sensitive systems should use stronger authentication methods).

Please refer to *CNCS Cybersecurity Control Families* for further details regarding established CNCS measures for identification and authentication.

3.3.9. Incident Response (IR)

CNCS has developed and formally documented the *CNCS Incident Response Plan,* as amended. The plan, is reviewed annually and updated, as necessary, to ensure its applicability to the CNCS environment and compliant with applicable federal laws, directives and policies, regulations, standards, and guidance.

Please refer to the *CNCS Incident Response Plan* for further details regarding established CNCS measures for incident reporting and handling.

3.3.10. Maintenance (MA)

CNCS information system resources are maintained in accordance with industry best practices, as applicable, to ensure their availability, integrity, and confidentiality. CNCS will schedule, perform, document, and review routine and preventative maintenance, as well as repairs on each system and component, in accordance with manufacturer or vendor specifications.

Please refer to *CNCS Cybersecurity Control Families* for further details regarding established CNCS measures for system maintenance.

3.3.11. Media Protection (MP)

CNCS data is stored on a variety of acceptable media and must be protected from unauthorized disclosure, damage, fraud, and abuse. To protect the security and privacy of information, CNCS will use a variety of security mechanisms that provide protections for media, and provide employees with guidance as to how IT property is purchased, installed, loaned, tracked, and disposed of by the agency.

Please refer to the *CNCS Cybersecurity Control Families* for further details regarding media protection and management.

3.3.12. Physical and Environmental Protection (PE)

CNCS will limit physical access to information systems, equipment, and the respective operating environments to authorized individuals. Administrative, physical, and technical safeguards must be applied; and can include the use of locks, guards, administrative controls, and measures to protect against damage from intentional acts, accidents, fires, and environmental hazards.

Please refer to the *CNCS Cybersecurity Control Families* for further details regarding physical and environmental protection.

3.3.13. Planning (PL)

Systems have increasingly taken on a strategic role in the organization. They assist organizations in conducting their daily activities and support decision making. Planning for systems is crucial in the development and implementation of the organization's information security goals.

NIST 800-53, as amended, requires all systems and applications have a documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and documented procedures to facilitate the implementation of the security planning policy and associated security planning controls. Accordingly, all CNCS systems must have a documented System Security Plan (SSP).

CNCS has developed and formally documented a process to ensure CNCS IT investments are aligned with business strategies, in *Information Technology Capital Planning and Investment Control (CPIC),* as amended. The policy is reviewed annually and updated, as necessary, to ensure it is applicable to the CNCS environment and compliant with applicable federal laws, directives and policies, regulations, standards, and guidance.

Please refer to *CNCS Cybersecurity Control Families* for further details regarding CNCS established policy and procedures for system security planning.

3.3.14. Personnel Screening for Information and Information System Access (PS)

Access to CNCS information resources is to be limited to only those persons who have been appropriately screened and authorized. CNCS will ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions, ensure that information resources are protected during and after personnel actions, employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Please refer to *CNCS Cybersecurity Control Families* for further details regarding CNCS established policies and procedures for personnel screening.

3.3.15. Risk Assessment (RA)

CNCS will follow NIST SP 800-39, *Managing Information Security Risk Organization, Mission and Information System View*, as the guidance for a risk-based approach to determine information security requirements to ensure that security is commensurate with the risk and magnitude of harm that can result from the loss, misuse, unauthorized access to, or modification of, CNCS information. Risk management procedures must be integrated into the System Development Lifecycle (SDLC) for each CNCS information resource. Security considerations must be included in the initiation, development/acquisition, implementation, operation/maintenance, and disposal of all CNCS information resources.

Please refer to the *CNCS Cybersecurity Control Families* for further details regarding CNCS policy and procedures for risk management.

3.3.16. System and Services Acquisition (SA)

Security requirements and specifications must be included, either explicitly or by reference, in all CNCS contracts, and solicitations for contracts, for information systems and information services and has the proper FAR clause language to cover the vendor requirements to implement a set of cybersecurity measures to attain the basic safeguarding security and privacy controls in accordance to FAR part 52.204-21 determine if the system is a covered contractor information system NIST SP 800-171, FISMA of 2014, and other applicable statutory, regulatory and policy requirements. The security requirements specified for the contract should be based on an assessment of risk for the contract and the Federal Information Processing Standards (FIPS) 199 security category of the system covered by the contract.

Please refer to the *CNCS Cybersecurity Control Families* for further details regarding established CNCS measures for system and service acquisitions.

3.3.17. System and Communications Protection (SC)

CNCS monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Please refer to the *CNCS Cybersecurity Control Families* for further details regarding system boundary protection.

3.3.18. System and Information Integrity (SI)

CNCS will adhere to patch management and maintenance guidance as set forth in NIST SP 800-40, *Guide to Enterprise Patch Management Technologies*, and subsequent publications. CNCS performs periodic and timely maintenance on organizational information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information

system maintenance. Patches are deployed to proactively prevent the exploitation of vulnerabilities in CNCS systems.

Please refer to the *CNCS Cybersecurity Control Families* for further details regarding system integrity.

4.0 CLOUD COMPUTING

Cloud computing is a model for enabling secure, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing allows CNCS to conveniently rent access to computing infrastructure assets, fully featured applications, software development and deployment environments. CNCS is committed using a cloud solution as its first choice for an IT modernization solution. As such, this requires additional review to determine the overall security being offered by a cloud service provider (CSP).

CNCS will use NIST guidance to manage the cloud computing program.

4.1. Cloud Service

CNCS defines a cloud service as a procured need that meets a specific business requirement that is hosted in a cloud environment. This cloud service can be managed directly by CNCS through OIT or contracted by the business unit requiring the service. CNCS shall maintain an accurate inventory of all cloud services maintained directly by CNCS or through a contracted service by business unit requiring service.

All contracts and procurements of cloud services must utilize standardized contract language, including Statements of Work (SOW) and any other contract sections and clauses as deemed appropriate to ensure vendors agree to comply with federal mandates for IT systems, such as cyber security protections, FISMA compliance, and federal records management.

4.1.1. Infrastructure as a Service (IaaS)

Infrastructure as a Service is service model where the CSP provides the computing resources (e.g., servers, storage, etc) and ensures those resources are available. CNCS is able to manage and control those resources in the same manner as if they were physically located at CNCS. Beyond providing the physical resources in a cloud environment and ensuring those resources are continuously available, the CSP has a reduced security responsibility. CNCS as a customer shall be responsible for all applications and software security within the environment.

4.1.2. Platform as a Service (PaaS)

Platform as a Service is a service model where the CSP manages and controls the underlying infrastructure. However, CNCS as a customer is able to create or load applications in the cloud environment. Maintaining the proper security for the PaaS is a shared responsibility between the CSP and CNCS. The CSP is responsible for the security aspects of the infrastructure (e.g. servers, switches, etc); CNCS shall be responsible for security aspects of the application.

4.1.3. Software as a Service (SaaS)

Software as a Service is service model where the CSP manages and controls the underlying infrastructure and the application. The CSP is ultimately responsible for all security aspects of the service. CNCS as a customer uses the service provided by the software; therefore, no additional configuration or management is required. In some instances, CNCS may be able to manage the access levels of the accounts on the service. Table 3: CSP vs CNCS Security Responsibilities provides a summary of the security responsibilities as it relates to a cloud service.

Table 3: CSP vs CNCS Security Responsibilities

Service	CSP Security Level of Responsibility	CNCS Security Level of Responsibility
IaaS	Low – covers the actual computing resources and their availability	High – covers operating systems and any software
PaaS	Shared – all aspects related to the environment (e.g. servers, operating system, storage, etc.)	Shared – loaded or created applications
SaaS	High – all aspects of the cloud environment	Low- account access to the service

4.2. Choosing a CSP

CNCS will attempt to use when practicable and within budget and functional constraints, a Federal Risk and Authorization Management Program (FedRAMP) authorized CSP. The benefits of using a FedRAMP CSP are:

- Increases reuse of existing security assessments across agencies
- Saves significant cost, time and resources – do once, use many times
- Provides enhanced security visibility through standardized continuous monitoring reports and monthly reviews of CSP vulnerabilities
- Supports risk-based security management
- Provides transparency between government and CSPs
- Improves trustworthiness, reliability, consistency, and quality of the Federal Government security authorization process

If a FedRAMP CSP that meets CNCS's functional requirement is not available, CNCS will consider non-FedRAMP CSP options. CNCS Cybersecurity will conduct a security review of a CSP to ensure it meets, at a minimum, the following security concerns that include bur are not limited to:

- Information Security Management Program
- Availability
- Physical Security
- Infrastructure

- Mobile Security / Mobile Access
- Operating System Platform
- Supported Browsers
- Authentication & Authorization
- Configuration Management (CM)
- Vulnerability Scanning & Penetration Testing
- Data Protection[12]
- Privacy Policy
- Service Level Agreements (SLAs)

The results of this security review will be used to make a risk based decision in accordance CNCS SDLC policy on whether or not to pursue the procurement of the cloud service by a non-FedRAMP CSP.

4.3. Cloud Authorization

A number of factors affect how CNCS will authorize the usage of a cloud service. CNCS is responsible for ensuring any cloud service is structured to protect the security of any CNCS information.

4.3.1. FedRAMP CSP Authorization

CNCS will utilize existing authorization for FedRAMP CSPs. However, CNCS is required to conduct due diligence on any FedRAMP CSP because the CSP may not fully address all of the security controls required. In those instances CNCS will at a minimum:

1. Review the CSP FedRAMP authorization package.
2. Identify all controls that the CSP does not fully address, to include any privacy controls.
3. Determine if security controls are addressed by common control.
4. Document any remaining security controls and CNCS responsibility for addressing those security controls[13].

[12] Additional security is required if CNCS will use the CSP to store, manage, or transmit personally identifiable information (PII).

[13] Documentation could be either a SSP, standard operating procedure (SOP), or an authorization memo.

4.3.2. Non-FedRAMP CSP Authorization

For non-FedRAMP CSPs, depending on the service, CNCS will at minimum:

- Determine if the CSP has any creditable cloud certifications[14]
- If necessary, ask the CSP to complete a cloud security self-assessment. The completion of the self-assessment will assist CNCS in identifying non-compliant security controls
- Identify the risk of any non-compliant security controls
- Work with the CSP to create a way to mitigate the risk
- Document the mitigation plan and CNCS responsibilities[15]

4.3.3. Issuing an Authorization

The CSP service's designation as either FedRAMP or non-FedRAMP will determine how CNCS will issue an authorization.

Table 4: CSP Authorization

CSP	IaaS	PaaS	SaaS
FedRAMP	ATO or OA - will require SSP, POAM, and SAR	ATO or OA – will require SAR and may require documentation* defining unaddressed security controls and usage procedures	ATO or OA – may require SAR and may require documentation* defining usage
Non-FedRAMP	ATO or OA - will require SSP, POAM, and SAR	ATO or OA – will require SAR and may require documentation* defining unaddressed security controls and usage procedures	ATO or OA – may require SAR and may require documentation* defining usage

*The CSP usage will govern the level of documentation required.

[14] A cloud certification is where the CSP has conducted and applied the industry accepted practices for securing a cloud environment. The most notable one is Cloud Security Alliance.
[15] Documentation could be either a SSP, standard operating procedure (SOP) or an authorization memo

4.4. Cloud Inventory

CNCS is required to fully document all cloud services in the same method as information systems. Cybersecurity will maintain the following information on all cloud services:

- Name of cloud CSP
- Type of cloud service (i.e., SaaS, PaaS, IaaS)
- Description of cloud service being provided, this should include the business requirement
- Office using the cloud service
- Authorization status (e.g., FedRAMP, non-FedRAMP, OA, etc)
- URL, if applicable
- Access to service level agreement
- CSP Point of Contact

APPENDIX A: Applicable Laws and References

This Cybersecurity Policy is in accordance with laws, directives, Executive Orders, requirements, and guidance that include the following:

- 44 U.S.C. § 3501, et. seq.; 44 U.S.C. §§ 3601-3606 (E-Government Act of 2002 (Pub. L. 107–347 (2002))
- 44 U.S.C. § 3551 et seq. Public Law (P.L.) 113-283 (*Federal Information Security Modernization Act 2014* (FISMA)) (as amended)
- 18 U.S.C. § 1030 (*Computer Fraud and Abuse Act)*
- 5 U.S.C. § 552a (*The Privacy Act of 1974*)
- FAR part 52.204-21
- Standards prescribed under 40 U.S. C. § 11331.
- OMB Memorandum, A-130, *Managing Information as a Strategic Resource*, July 2016
- OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act*, December 23, 2016
- OMB A-123, *Management's Responsibility for Enterprise Risk Management and Internal Contro*l (July 2016),
- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017
- OMB Memorandum M-17-09, *Management of Federal High Value Assets*, December 9, 2016
- OMB Memorandum, M-16-24, *Role and Designation of Senior Agency Official on Privacy*, September 2016
- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 2015
- OMB Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*, November 4, 2016
- OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 2013
- OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Modernization Act 2014 and Agency Privacy Management*, September 2012
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006
- OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003
- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 500-29, Version 2, *Cloud Computing Standards Roadmap*, July 2013
- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*
- NIST SP 800-16 (as amended), *A Role-Based Model for Federal Information Technology / Cyber Security Training*
- NIST SP 800-39 (as amended), *Managing Information security Risk: Organization, Mission, and Information System View*

- NIST SP 800-40 (as amended), *Guide to Enterprise Patch Management Technologies*
- NIST SP 800-53 (as amended), *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A (as amended), *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*
- NIST SP 800-60 Volume I Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-60 Volume II Revision 1, *Appendices to Volume I, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61 (as amended), *Computer Security Incident Handling Guide*
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*
- NIST SP 800-137 (as amended), *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*
- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- NIST SP 800-171, *Protecting Controlled Unclassified information in Nonfederal Information Systems and Organizations*

APPENDIX B: Acronyms and Abbreviations

Acronym	Acronym Definition/Name/Title
AO	Authorizing Official
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CNCS	Corporation for National & Community Service
COO	Chief Operating Officer
COR	Contracting Officer's Representative
CSP	Cloud Service Provider
FISMA	Federal Information Security Modernization Act 2014Act
FOIA	Freedom of Information Act
IA	Information Assurance
IaaS	Infrastructure as a Service
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
NARA	National Archives and Records Administration

Acronym	Acronym Definition/Name/Title
NIST	National Institute of Standards & Technology
OGC	Office of General Counsel
OHC	Office of Human Capital
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPS	Office of Personnel Security
PaaS	Platform as a Service
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POAM	Plan of Action and Milestones
POC	Point of Contact
ROB	Rules of Behavior
SaaS	Software as a Service
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SDLC	System Development Lifecycle

Acronym	Acronym Definition/Name/Title
SORN	System of Records Notice
SP	Special Publication
SSP	System Security Plan
SSN	Social Security Number
ST&E	Security Test and Evaluation
VPN	Virtual Private Network